

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION**

NETJETS AVIATION, INC., et al.,

Plaintiffs,

v.

**Civil Action 2:22-cv-2417
Judge James L. Graham
Magistrate Judge Jolson**

STEPHEN G PERLMAN, et al.,

Defendants.

ORDER

This matter is before the Court on Defendants’ Motion for Reconsideration of the Court’s Order (Doc. 96) Concerning the Sealing of Trust Documents and Brokerage Statements. (Doc. 99). Because Defendants’ request is not narrowly tailored, the Motion is **DENIED**.

I. BACKGROUND

This is the latest in Defendants’ quest to seal documents for the parties’ upcoming dispositive motions. On June 21, 2024, Defendants filed their first unopposed motion to seal various documents. (Doc. 78). Because Defendants failed to meet the requirements for sealing, the Court denied that motion without prejudice. (Doc. 84). Defendants re-filed that motion on July 10, 2024. (Doc. 90). After reviewing the motion and the documents at issue, the Court only partially granted the motion. (Doc. 96).

Most relevant here, the Undersigned denied Defendants’ request to seal two versions of the Perlman Trust declarations and two brokerage statements. (*Id.* at 6–9). For the declarations, Defendants argued the documents could be used for identity verification purposes, and disclosure would put Defendant Perlman at risk for hacking attempts. (*Id.* at 6). As to the brokerage

statements, Defendants represented that the existence of these accounts had never been revealed publicly, and doing so would make them targets for hackers. (*Id.* at 9). The Court denied the requests to seal the documents wholesale but allowed Defendants to make further redactions to protect Defendant Perlman’s security interests. (*Id.* at 6–9). In doing so, the Court noted the documents’ relevance to this case. (*Id.* at 6 (“As this Court previously explained, the trust documents are highly relevant for Plaintiffs’ alter ego claims.” (citing Doc. 84 at 6–7; Doc. 67 at 2))). The Court also highlighted that Defendants had not provided any examples where trust instruments were sealed by a court in their entirety or where hackers used a trust instrument to access a financial account. (*Id.* at 7). At base, the Court found Defendants’ request was not narrow enough to serve Defendant Perlman’s asserted security interests. (*Id.* at 8–9).

Now, Defendants ask the Court to reconsider that decision. (Doc. 99 (motion for reconsideration); Doc. 101 (supplemental memorandum in support of the motion)). Specifically, Defendants again move to seal the trust declarations and the brokerage statements, which they previously provided to the Court for *in camera* review. (*See generally* Doc. 99). After reviewing those documents once more, the motion is ripe for the Undersigned’s review. (Docs. 99, 101).

II. DISCUSSION

“As a general principle, motions for reconsideration are looked upon with disfavor unless the moving party demonstrates: (1) a manifest error of law; (2) newly discovered evidence which was not available previously to the parties; or (3) intervening authority.” *Meekison v. Ohio Dep’t of Rehab. & Corr.*, 181 F.R.D. 571, 572 (S.D. Ohio 1998) (citing *Harsco Corp. v. Zlotnicki*, 779 F.2d 906, 909 (3d Cir. 1985), *cert. denied*, 476 U.S. 1171 (1986)). Defendants say new evidence shows that the trust declarations and brokerage statements must be sealed in their entirety to protect Defendant Perlman from hackers and other bad actors. (Doc. 99 at 2).

“‘[T]he public has a strong interest in obtaining the information contained in the court record.’” *Shane Grp., Inc. v. Blue Cross Blue Shield of Mich.*, 825 F.3d 299, 305 (6th Cir. 2016). (quoting *Brown & Williamson Tobacco Corp. v. F.T.C.*, 710 F.2d 1165, 1180 (6th Cir. 1983)). As a result, the Court “has an obligation to keep its records open for public inspection [and] that obligation is not conditioned upon the desires of the parties to the case.” *Harrison v. Proctor & Gamble Co.*, No. 1:15-cv-514, 2017 WL 11454396, at *1–2 (S.D. Ohio Aug. 11, 2017) (citing *Shane Grp., Inc.*, 825 F.3d at 307). For this reason, a party seeking to seal records has a “heavy” burden of overcoming a “‘strong presumption in favor of openness’ as to court records.” *Shane Grp., Inc.*, 825 F.3d at 305 (quoting *Brown & Williamson*, 710 F.2d at 1179).

“[I]n civil litigation, only trade secrets, information covered by a recognized privilege (such as the attorney-client privilege), and information required by statute to be maintained in confidence (such as the name of a minor victim of a sexual assault), is typically enough to overcome the presumption of access.” *Id.* at 308 (citation and quotations omitted). To overcome “the strong presumption in favor of openness,” parties who move to seal documents must demonstrate: “(1) a compelling interest in sealing the records; (2) that the interest in sealing outweighs the public’s interest in accessing the records; and (3) that the request is narrowly tailored.” *Kondash v. Kia Motors Am., Inc.*, 767 F. App’x 635, 637 (6th Cir. 2019).

Defendants provide three pieces of evidence in support of their renewed request to seal. First, they say that Mr. Perlman’s personal information was released in a recent AT&T data breach, along with 73 million other account holders. (Doc. 99 at 3). Second, Defendants offer a report from Jack Bicer, who “has a 40-year career in software development” and is an expert on various cybersecurity-related topics. (*Id.* at 2–3; Doc. 99-1). Third, they represent Defendant Perlman recently received “eight emails from Experian IdentityWorks, each notifying him that his social

security number had been identified on the dark web.” (Doc. 101 at 1–2). Based upon this evidence, Defendants argue the documents at issue must be sealed to prevent hacks and “severe and irreparable damage” to Defendant Perlman. (*See* Doc. 99 at 6–7).

Previously, Defendants provided information to the Court about why revealing certain personal information puts Defendant Perlman at risk of hacking:

[Account takeover fraud (ATO)] results from hackers getting access to sensitive personal identifying information. As a result of repeated hacks of large corporations,[] basic personal identifying information of most Americans, such as social security number, mother’s maiden name, birth date, etc., are readily available to hackers on the dark web.[] Because it can be readily obtained by bad actors, such basic personal identification information is no longer sufficient to authenticate an individual’s identity.

Financial institutions, as well as other institutions requiring high security, rely upon a method of high-level authentication called “Dynamic Knowledge-based Authentication” or “Dynamic KBA”.[] In general, knowledge-based authentication (“KBA”) “is a method of authentication which seeks to prove the identity of someone accessing a service such as a financial institution or website.” *Id.* There are two types of KBA: static KBA and Dynamic KBA. Static KBA is “based on a pre-agreed set of shared secrets[.]” *Id.* For example, security questions such as “where did you meet your spouse,” would qualify as static KBA. *Id.* Dynamic KBA is based on questions generated from a wider base of personal information.” *Id.*

(Doc. 90 at 6 (cleaned up)).

Defendants again claim the trust declarations and brokerage statements could be used as dynamic KBA to access Defendant Perlman’s financial accounts. (*Compare id.* at 11–13 (stating disclosure of the brokerage statements and trust documents could be used to verify Defendant Perlman’s identity and could put him at greater risk for hacking) *with* Doc. 99 (same)).

After reviewing Defendants’ new evidence, the Court finds not much has changed. To begin, Defendants previously briefed the issue of dynamic KBA, and the Court considered those arguments in its past decision. (Doc. 96 at 6 (noting Defendants’ arguments about dynamic KBA and their assertion that the Code of Federal Regulations allows institutions to use trust instruments

to verify identities)). In that decision, the Court also acknowledged that Defendant Perlman has been a hacking victim in the past, and like millions of others, it appears his information continues to be exposed. (*See* Doc. 96 at 4 (referencing a previous security breach that affected Defendant Perlman); Doc. 99 at 3 (discussing a data breach that included 73 million accounts); Doc. 101 at 2 n.1 (discussing another data breach that impacted potentially three billion individuals, including Defendant Perlman)). These facts alone do not warrant entirely sealing the documents at issue. Defendant Perlman is not alone in having his personal information exposed on the dark web or to other bad actors. (*See* Doc. 90 at 7–8 (discussing that most people’s basic personal information is available to bad actors already)). So, if these types of breaches were enough, all individuals participating in litigation could seal vast swaths of documents they believe could be used to verify their identity.

Even so, Defendants rely on the report of Mr. Bicer to show that information contained in the trust declarations place Defendant Perlman at an elevated risk of hacking. Specifically, Mr. Bicer asserts that financial “institution[s] will assume the Trust instrument has never been disclosed publicly,” so portions of the declarations could be used “by a hacker to fraudulently verify to the bank or other institution the hacker posing as Mr. Perlman.” (*Id.* at 7 (explaining that language in the trust declarations can be used as dynamic KBA)). But again, Defendants and Mr. Bicer do not provide a single example or cite a case where a trust declaration has been used for this purpose. *See Shane Grp., Inc.*, 825 F.3d at 305–06 (stating movants must provide “reasons and legal citations” for sealing documents). Instead, they offer examples where hackers have bribed employees and used SIM card swaps to hack email accounts and cell phones. (Doc. 99-1 at 6–7). In one of those examples, hackers used an individual’s “account information, email and phone number” for their attack, which the Court has already allowed Defendant Perlman to redact.

(Doc. 96 at 8 (allowing family members’ names, addresses, and contact information to be redacted from the trust declarations); *id.* at 9 (granting redactions for account names, addresses, and other financial information)). Accordingly, none of these examples are particularly relevant to the risk Defendants speculate about here.

In addition, Defendants’ request is still not narrowly tailored. Defendants do not explain “line-by-line” why the documents must be sealed. *Shane Grp., Inc.*, 825 F.3d at 308. Nor do they cite “cases where courts have allowed entire trust instruments to be sealed.” (Doc. 96 at 7). Instead, Mr. Bicer says that nearly all the information in the trust declarations could be used to verify Defendant Perlman’s identity. (Doc. 99-1 at 7–8). Again, the Court finds this argument unpersuasive, since Defendants cannot point to a single instance where, for example, “[t]he exact wording of titles,” “introductory clauses,” or “[s]pecific words and phrases” from a trust instrument were used to hack a financial account. (*See id.*).

What’s more, these documents are already heavily redacted. For example, Bates Stamp FED002158–61 includes only Defendant Perlman’s name, the date the Trust was entered into, and standard language included in nearly every trust. Take, for example, this unredacted section:

The Settlor has transferred to the Trustee, without consideration, the property described on Schedule “A” attached hereto and made a part hereof. All such property and all property transferred to this Trust in the future shall constitute the “Trust Estate,” which shall be held, managed and distributed according to the terms of this Declaration. The Trustee accepts such title to the Trust Estate as is conveyed or transferred to the Trustee hereunder without liability for the condition or validity of such title.

(Bates Stamp FED002158).

Even considering Mr. Bicer’s report, the Court cannot ascertain why this language must be sealed to prevent hacking. True, the other version of the trust declaration is somewhat less redacted. Yet large segments contain only boilerplate language, like paragraphs about settlor

duties and powers. (*See* Bates Stamp FED30749–50). Plus, the portions that include more personal information, like the particulars of distributions and gifts, are already heavily redacted. (Bates Stamp FED30751–53). More still, the Court already ordered that Defendant could redact these documents further to shield financial and other personal information. (Doc. 96 at 8–9). The Court again finds these redactions are sufficient to protect Defendant Perlman’s security interests and uphold the Court’s obligation to keep its records open to the public. (*See* Doc. 96 at 6–9 (discussing the relevance of these documents to the case, addressing Defendants’ security concerns, and allowing further redactions)).

Turning to the brokerage statements, Mr. Bicer asserts these documents must be sealed because “the fact that Mr. Perlman has assets at these brokerage firms has never been publicly released before.” (Doc. 99-1 at 8). Again, while that may be true, “these documents may also be relevant in showing any financial connections between Defendants Perlman and the Trust.” (Doc. 96 at 9). And, again, the Court has already allowed redactions of account information, personal addresses, and account totals for these documents. (*Id.*).

At base, Defendants’ request is not narrowly tailored. If Defendants wish to redact more than what the Court has previously allowed, they must propose those redactions line-by-line, file a motion to seal pursuant to *Shane Group*, and demonstrate why those redactions are warranted. *Shane Grp., Inc.*, 825 F.3d at 305–06 (“[E]ven where a party can show a compelling reason why certain documents or portions thereof should be sealed, the seal itself must be narrowly tailored to serve that reason. . . . The proponent of sealing therefore must analyze in detail, document by document, the propriety of secrecy, providing reasons and legal citations.” (internal quotations and citations omitted)). For these reasons, Defendants’ Motion is **DENIED**.

III. CONCLUSION

For the foregoing reasons, Defendants' Motion for Reconsideration (Doc. 99) is **DENIED**.

IT IS SO ORDERED.

Date: September 5, 2024

/s/ Kimberly A. Jolson
KIMBERLY A. JOLSON
UNITED STATES MAGISTRATE JUDGE